



# The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

**SAFER • HEALTHIER • PEOPLE™**



# Provisions



- Sets boundaries on the use/release of health records
- Holds violators accountable with penalties
- Strikes a balance when public health responsibilities support disclosure of certain forms of data
- Enables patients to find out how their information may be used and what disclosures of their information have been made
- Gives patients the right to obtain a copy of their own health record and request corrections



# Covered Entities

Entities covered under the HIPPA  
Privacy Rule include:

- Health Plans
- Healthcare clearinghouses
- Healthcare providers who conduct certain administrative and financial transactions electronically



# Impact on Public Health

- The Privacy Rule expressly permits protected health information (PHI) to be shared for specified public health purposes
- Covered entities may disclose PHI without individual authorization to a public health authority legally authorized to collect/receive information for the purpose of preventing or controlling disease, injury, or disability



# What disclosures are permitted without authorization?

- Required by law
- Public health surveillance, investigations and interventions
- Abuse, neglect, or domestic violence
- Law enforcement
- Oversight
- Workers compensation

For a full list, please visit <http://www.hhs.gov/ocr/hipaa>



# Are Public Health Authorities considered Business Associates?

- Under the HIPAA Privacy Rule, business associates include: lawyers, accountants, billing companies, and other contractors whose relationship with covered entities requires sharing of PHI.
- Public health authorities receiving information from hospitals (covered entities) are not business associates and therefore are not required to enter into business associate agreements.



# Patient identifiers sent to NGSN include...

- Patient ID number
- Admission date
- Gender
- Date of birth
- Surgery date
- Operative procedure



# Accounting for Public Health Disclosures



- Accounting of disclosure NOT required for:
  - For treatment payment and healthcare operations (TPO)
  - Pursuant to the individual's written authorization
- Accounting of disclosures required if no authorization was made – includes disclosures to Public Health





# Accounting of Disclosure Requirements



- Each accounting would include:
  1. Type of disclosure
  2. Date of disclosure
  3. Identity (with address) of the recipient
  4. Brief description of protected health information disclosed
  5. Purpose of the disclosure



# Required accounting of disclosures

- In NHSN, disclosures can be quickly identified through one of the following methods:
  - Search for the patient by name. All reported events and procedures for that patient are available for an unlimited time period, including the specific PHI that was reported to NHSN
  - Run line lists of Events and Procedures by a specific time period (e.g., month, quarter). A complete documentation of PHI reported to NHSN can be generated



# Summary

- NHSN is a Public Health Entity
- The Privacy Rule expressly permits PHI to be shared for public health purposes without individual authorization
- NHSN is not a business associate and business agreements are not made with hospitals
- Accounting of disclosures to NHSN are required and can be generated at any time in the NHSN application



# Additional Resources

- Office for Civil Rights – HIPAA:  
<http://www.hhs.gov/ocr/hipaa/>
- HIPAA Privacy Rule and Public Health - Guidance from CDC and the U.S. Department of Health and Human Services:  
<http://www.cdc.gov/mmwr/preview/mmwrhtml/su5201a1.htm>
- HIPAA Disclosures for Public Health Activities:  
<http://www.hhs.gov/ocr/hipaa/publichealth.pdf.pdf>